Sets of lengths of integer-valued polynomials

Sarah Nakato

(joint work with Sophie Frisch and Roswitha Rissner)

AWMA Virtual Seminar

October 26, 2023

FWF
Der Wissenschaftsfonds.

KABALE UNIVERSITY
KAB
KNOWLEDGE IS THE FUTURE

Introduction

- A ring R is a non-empty set together with two operations, usually $+$ and $\times$, satisfying certain properties, e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $R[x] = \{f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R\}$.
- Every non-zero integer except 1, and -1 can be expressed uniquely as a product of prime numbers. We say that $\mathbb{Z}$ has uniqueness of factorization of elements.
- Not all rings have uniqueness of factorization of elements. For instance, in

$$\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\},$$

$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Fermat's Last Theorem

For $n \geq 3$, $x^n + y^n = z^n$, has no non-trivial solutions $x, y, z \in \mathbb{Z}$.

Introduction

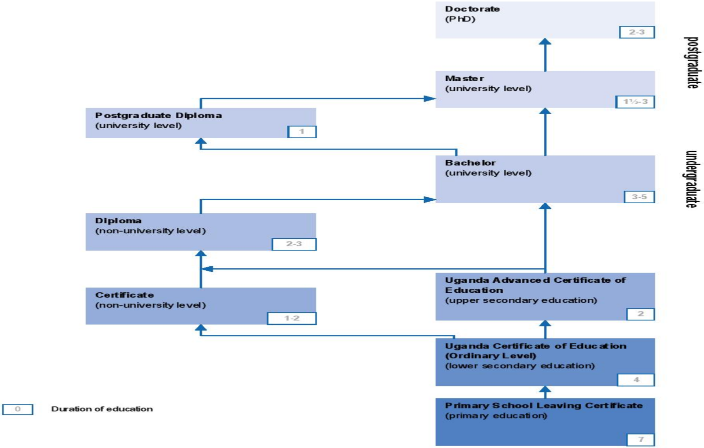
- Factorization theory involves investigating phenomena related to non-uniqueness of factorizations in algebraic structures.
- To characterize arithmetical and algebraic properties of algebraic structures in terms of factorization properties.
- Sets of lengths are the most studied objects in factorization theory.

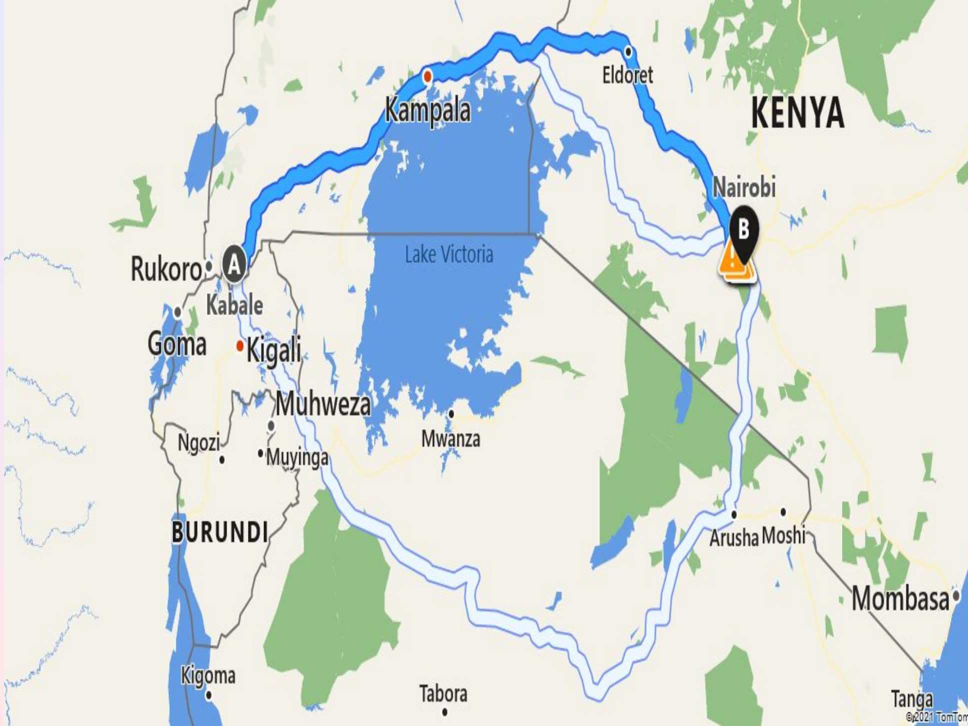
Introduction

Remark 1

In real life, non unique factorizations tell us that there can be other ways of doing something or achieving a goal. For instance, the different academic paths.

Flow chart: education system Uganda




KENYA
Eldoret
Kampala
Nairobi
B
A
Rukoro
Kabale
Lake Victoria
Goma
Kigali
Muhweza
Ngozi
Muyinga
Mwanza
BURUNDI
Arusha
Moshi
Mombasa
Kigoma
Tabora
Tanga

Outline

- Preliminaries on integer-valued polynomials and factorizations
- Sets of lengths in $\mathrm{Int}(D)$

Integer-valued polynomials

Definition 1

The ring of integer-valued polynomials is the ring

$$\mathrm{Int}(\mathbb{Z}) = \{\mathbf{f} \in \mathbb{Q}[\mathbf{x}] \mid \forall\ \mathbf{a} \in \mathbb{Z}, \mathbf{f}(\mathbf{a}) \in \mathbb{Z}\} \subseteq \mathbb{Q}[x].$$

For example, $2x+3$ is in $\mathrm{Int}(\mathbb{Z}) \rightsquigarrow \mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z})$. Also

$$f = \frac{1}{2}x^2 + \frac{1}{2}x = \frac{x(x+1)}{2} \in \mathrm{Int}(\mathbb{Z}).$$

Remark 2 (Cahen & Chabert, 2016)

A polynomial $f \in \mathbb{Q}[x]$ is in $\mathrm{Int}(\mathbb{Z})$ if

$$\mathbf{f}(\mathbf{a}) \in \mathbb{Z} \ \text{ for all } \ \mathbf{0} \leq \mathbf{a} \leq \deg(\mathbf{f}),$$

e.g., $f = \frac{x^2+x+3}{3} \notin \mathrm{Int}(\mathbb{Z})$ since $f(1) = \frac{5}{3} \notin \mathbb{Z}$.

More examples

1. $f = \frac{x^2+x+2}{2} \in \mathrm{Int}(\mathbb{Z})$ since $f(0) = 1, f(1) = 2$, and $f(2) = 4$.
2. A product of n consecutive integers is divisible by $n!$, e.g.,

$$\frac{x(x+1)(x+2)}{6} \in \mathrm{Int}(\mathbb{Z}).$$

   - Each binomial polynomial

$$\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!} \in \mathrm{Int}(\mathbb{Z}).$$

3. For each prime number p, the Fermat's polynomial

$$\frac{x^p - x}{p} \in \mathrm{Int}(\mathbb{Z}) \quad \Longleftarrow \quad a^p \equiv a \pmod{p} \ \ \forall\ a \in \mathbb{Z},$$

e.g., $\frac{x^7-x}{7} \in \mathrm{Int}(\mathbb{Z})$.

Integer-valued polynomials on arbitrary domains

Definition 2

Let D be a domain with quotient field K. The ring of integer-valued polynomials on D is

$$\mathbf{Int(D) = \{f \in K[x] \mid \forall\, a \in D, f(a) \in D\}} \subseteq K[x]$$

Remark 3

1. For all $f \in K[x]$, $f = \frac{g}{b}$ where $g \in D[x]$ and $b \in D \setminus \{0\}$.
2. $f = \frac{g}{b}$ is in $\mathrm{Int}(D)$ if and only if $b \mid g(a)$ for all $a \in D$.

For example, $D[x] \subseteq \mathrm{Int}(D)$.

Int(D) cont'd

- Int($\mathbb{Z}$) is non-Noetherian.
- Int(D) in general is not a unique factorization domain e.g., in Int($\mathbb{Z}$),

$$\begin{aligned} x^2 + x &= x \cdot (x+1) \\ &= 2 \cdot \frac{x(x+1)}{2} \end{aligned}$$

$$\begin{aligned} \frac{(x-1)(x-2)(x-3)}{2} &= (x-1) \cdot \frac{(x-2)(x-3)}{2} \\ &= (x-3) \cdot \frac{(x-1)(x-2)}{2} \end{aligned}$$

Factorization terms

Let R be a commutative ring with identity.

1. A non-zero element $u \in R$ is called a **unit** if there exists $b \in R$ such that $ub = 1$, e.g., the units of $\mathbb{Z}$ are $\{1, -1\}$.

2. A non-zero non-unit $r \in R$ is said to be **irreducible** in R if whenever $r = ab$, then either a or b is a unit, e.g., prime numbers are irreducible in $\mathbb{Z}$.

3. A **factorization** of r in R is an expression

$$r = a_1 \cdots a_n$$

where $n \geq 1$ and a_i is irreducible in R for $1 \leq i \leq n$.

Factorization terms cont'd

1. The **length** of the factorization $r = a_1 \cdots a_n$ is the number of irreducible factors n.

2. We say that $r, s \in R$ are **associated** in R if there exists a unit $u \in R$ such that $r = us$. We denote this by $\mathbf{r} \sim \mathbf{s}$, e.g., $3 \sim -3$ in $\mathbb{Z}$.

3. Two factorizations of the same element,

$$r = a_1 \cdots a_n = b_1 \cdots b_m, \tag{1}$$

are called **essentially the same** if $n = m$ and, after a suitable re-indexing, $a_j \sim b_j$ for $1 \leq j \leq m$. Otherwise, the factorizations in (1) are called **essentially different**.

Factorization terms cont'd

In $\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$,

- $6 = 2 \times 3 = -2 \times -3$ are essentially the same.
- $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are essentially different.

In $\mathbb{Z}[\sqrt{-14}] = \{m + n\sqrt{-14} \mid m, n \in \mathbb{Z}\}$,

- $81 = 3 \times 3 \times 3 \times 3 = -3 \times 3 \times -3 \times 3$ are essentially the same.
- $81 = 3 \times 3 \times 3 \times 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ are essentially different.

Factorization terms cont'd

1. The **set of lengths** of r is

$$L(r) = \{n \in \mathbb{N} \mid r = r_1 \cdots r_n\}$$

where $r_1, \ldots, r_n$ are irreducibles. e.g.,

In $\mathbb{Z}[\sqrt{-14}]$, $81 = 3 \times 3 \times 3 \times 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ are essentially different. $L(81) = \{2, 4\}$.

In $\mathrm{Int}(\mathbb{Z})$,

$$f = \frac{(x-1)(x-2)(x-3)}{2} = (x-1) \cdot \frac{(x-2)(x-3)}{2} = (x-3) \cdot \frac{(x-1)(x-2)}{2}$$

$L(f) = \{2, 2\} = \{2\}$.

Sets of lengths in $\mathrm{Int}(D)$

Theorem 1 (Frisch, 2013)

Let $1 < m_1 \leq m_2 \leq \cdots \leq m_n \in \mathbb{N}$. Then there exists a polynomial $H \in \mathrm{Int}(\mathbb{Z})$ with exactly n essentially different factorizations of lengths $m_1, \ldots, m_n$.

Say $\{2, 4, 5, 5\}$. Then there exists $H \in \mathrm{Int}(\mathbb{Z})$ such that

$$\begin{aligned} H &= h_1 \cdot h_2 \\ &= f_1 \cdot f_2 \cdot f_3 \cdot f_4 \\ &= e_1 \cdot e_2 \cdot e_3 \cdot e_4 \cdot e_5 \\ &= g_1 \cdot g_2 \cdot g_3 \cdot g_4 \cdot g_5 \end{aligned}$$

Corollary 1

Every finite subset of $\mathbb{N}_{>1}$ is a set of lengths of an element of $\mathrm{Int}(\mathbb{Z})$.

Sets of lengths in Int(D)

Question: Are there other domains D such that Int(D) has full system of sets of lengths? YES

If D is a Dedekind domain such that;

1. D has infinitely many maximal ideals and
2. $|D/M| < \infty$ for each maximal ideal M.

Then Int(D) has full system of sets of lengths.

Theorem 2 (Frisch, SN, Rissner, 2019)

Let $1 < m_1 \leq m_2 \leq \cdots \leq m_n \in \mathbb{N}$. Then there exists a polynomial $H \in \text{Int}(D)$ with exactly n essentially different factorizations of lengths $m_1, \ldots, m_n$.

Examples of our Dedekind domains

1. $\mathbb{Z}$.
2. Rings of integers of number fields, e.g., $\mathbb{Z}[\sqrt{-5}]$.

Transfer mechanisms

Several monoids with full system of sets of lengths have been obtained using transfer mechanisms. (Kainrath, 1999)

Definition 3

Monoids which allow transfer homomorphisms to block monoids are called transfer Krull monoids.

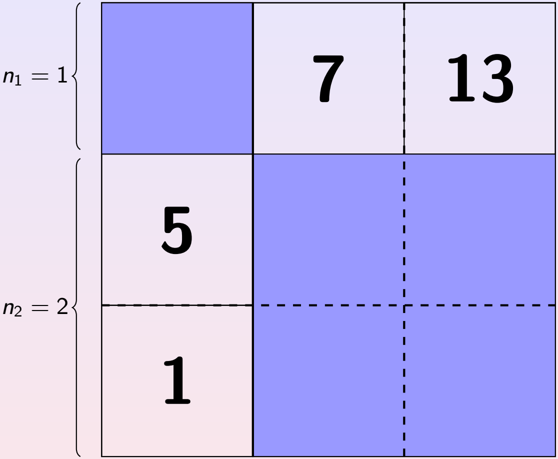
- $(\mathrm{Int}(\mathbb{Z}) \setminus \{0\}, \bullet)$ is not a transfer Krull monoid. (Frisch, 2013)
- $(\mathrm{Int}(D) \setminus \{0\}, \bullet)$ is not a transfer Krull monoid, where D is Dedekind domain with infinitely many maximal ideals of finite index. (Frisch, SN, Rissner, 2019)

I$\ell\ell$ustrations of tools

For $H \in \text{Int}(\mathbb{Z})$ with $L(H) = \{2, 3\}$, we start with $\{n_1, n_2\} = \{1, 2\}$.

1. $N = (\sum_{i=1}^{n} n_i)^2 - \sum_{i=1}^{n} n_i^2, \quad N = 4.$
2. Pick a prime number $p > N$. Say $p = 5$.
3. Construct a complete system of residues mod p that doesn't contain a complete system of residues mod any prime less that p, that is, from $\{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$, say $\mathcal{C} = \{5, 1, 7, 13, 19\}$.
4. Let $\mathcal{C} = S \uplus T$ such that $|T| = N$, Say $T = \{5, 1, 7, 13\}$, and set
$$s(x) = \prod_{r \in S} x - r = x - 19.$$

1. Arrange the elements of $T = \{5, 1, 7, 13\}$ in an $m = \sum_{i=1}^{n} n_i$ by m square matrix with diagonal blocks empty.



- $f_1^{(1)} = (x-7)(x-13)(x-5)(x-1)$
- $f_1^{(2)} = (x-5)(x-7), \quad f_2^{(2)} = (x-1)(x-13)$

- Set

$$h(x) = \frac{s(x) \cdot f_1^{(1)} \cdot f_1^{(2)} \cdot f_2^{(2)}}{p}.$$

- Replace each f_i with a corresponding monic irreducible polynomial F_i.
- $f_1^{(1)} = (x-7)(x-13)(x-5)(x-1)$

  $F_1^{(1)} = x^4 + 24x^3 + 16x^2 + 4x + 30$

- $f_1^{(2)} = (x-5)(x-7) \rightsquigarrow F_1^{(2)} = x^2 + 38x + 10$
- $f_2^{(2)} = (x-1)(x-13) \rightsquigarrow F_2^{(2)} = x^2 + 36x + 38$

Set

$$H(x) = \frac{s(x) \cdot F_1^{(1)} \cdot F_1^{(2)} \cdot F_2^{(2)}}{p}.$$

Then $H \in \mathrm{Int}(\mathbb{Z})$ and factors as

$$\begin{aligned} H(x) &= \frac{s(x) \cdot F_1^{(2)} \cdot F_2^{(2)}}{p} \cdot F_1^{(1)} \\ &= \frac{s(x) \cdot F_1^{(1)}}{p} \cdot F_1^{(2)} \cdot F_2^{(2)} \end{aligned}$$

References

1. Cahen Paul-Jean and Jean-Luc Chabert. **Integer-valued polynomials**. Vol. 48. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI,1997, pp. xx–322.

2. Cahen, Paul-Jean, and Jean-Luc Chabert. **What you should know about integer-valued polynomials.** The American Mathematical Monthly 123, no. 4 (2016), pp. 311-337.

3. Alfred Geroldinger and Franz Halter-Koch. **Non-unique factorizations.** Vol. 278. Pure and Applied Mathematics (Boca Raton). Algebraic, combinatorial and analytic theory. Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxii–700.

4. Florian Kainrath. **Factorization in Krull monoids with infinite class group.** Colloq. Math. 80.1 (1999), pp. 23–30.

References

5. Sophie Frisch. **A construction of integer-valued polynomials with prescribed sets of lengths of factorizations.** Monatsh. Math. 171.3-4 (2013), pp. 341–350.
6. **Sophie Frisch, Sarah Nakato, and Roswitha Rissner. Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields. *Journal of Algebra,* 528 (2019), pp. 231–249.**
7. Geroldinger, Alfred. **Sets of lengths.** *The American Mathematical Monthly* 123, no. 10 (2016), 960-988.
8. Fadinger-Held, Victor, Sophie Frisch, and Daniel Windisch. **Integer-valued polynomials on valuation rings of global fields with prescribed lengths of factorizations.** Monatshefte für Mathematik (2023), 1-17.